UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/067,319 | 02/07/2002 | Swati Deshmukh | 19903.0016 | 7037 |

23517 7590 02/12/2009

BINGHAM MCCUTCHEN LLP
2020 K Street, N.W.
Intellectual Property Department
WASHINGTON, DC 20006

| EXAMINER | |
|---|---|
| NGUYEN, QUANG N | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2441 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 02/12/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Application Number: 10/067,319
Filing Date: February 07, 2002
Appellant(s): DESHMUKH ET AL.

Kevin J. Zilka
For Appellant

**EXAMINER'S ANSWER**

This is in response to the Order Returning Undocketed Appeal to the Examiner from BPAI mailed 10/21/2008 and the Supplemental Appeal Brief filed 12/01/2008 appealing from the Final Rejection mailed 08/01/2006.

***(1) Real Party in Interest***

A statement identifying by name the real party in interest is contained in the brief.

***(2) Related Appeals and Interferences***

The examiner is not aware of any related appeals, interferences, or judicial proceedings, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

***(3) Status of Claims***

The statement of the status of claims contained in the brief is correct.

***(4) Status of Amendments After Final***

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

***(5) Summary of Claimed Subject Matter***

The summary of claimed subject matter contained in the brief is correct.

***(6) Grounds of Rejection to be Reviewed on Appeal***

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

Whether claims 1, 16-17, 32-33 and 48-81 are unpatentable under 35 U.S.C. 103(a) over U.S. Patent Application Publication 2003/0131256 to Ackroyd (Ackroyd) in view of U.S. Patent No. 6,493,755 to Hansen et al. (Hansen).

***(7) Claims Appendix***

The copy of the appealed claims contained in the Appendix to the brief is correct.

***(8) Evidence Relied Upon***

The following is a listing of the prior art of record relied upon in the rejection of claims under appeal:

**US 2003/0131256** to Ackroyd (Ackroyd) published on 07/10/2003.

**US 6,493,755** to Hansen et al. (Hansen) issued on 12/10/2002.

***(9) Grounds of Rejection***

The following ground(s) of rejection are applicable to the appealed claims:

***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**2. Claims 1, 16-17, 32-33 and 48-81 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ackroyd (US 200310131256 A1), hereinafter "Ackroyd", in view of Hansen et al. (US 6,493,755), hereinafter "Hansen".**

3. As to claim 1, **Ackroyd** teaches a method of reporting malware events, comprising the steps of:

detecting a plurality of malware events each with one of a plurality of levels using a malware scanner, the plurality of malware events comprising completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware *(**Ackroyd** teaches a malware policy organizing server 32 receiving logged data messages indicating defection of malware items/events by the malware scanners operating at various different servers and client computers, for example, the policy organizing server 32 has defected four logged data messages corresponding to a particular item of malware from computers running the*

*most up-to-date version of the virus definition data and also detects the pattern that none of these on innate from a computer running out-of data malware definition data, i.e., failure)* **(Ackroyd, paragraphs [0025] and [0030])**;

determining a level of a detected malware event *(i.e., identifying patterns of malware detection, for example, the malware scanners on a plurality of client computers detecting a particular Trojan infection occurring within computers connected to a particular department server 4)* **(Ackroyd, paragraphs [0027-0029] and [0032])**;

comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels *(at step 48, a determination is made as to whether or not any of the thresholds has been exceeded or any of the patterns matched)* **(Ackroyd, paragraphs [0027-0029])**; and

transmitting a notification of the detected malware event over a network, based on the comparison of the level of the detected malware event to the event trigger threshold *(if thresholds have been exceeded or patterns matched, then one or more predefined anti-malware actions are triggered and will be directed to the appropriate problem area within the network concerned and also making reports of this to the malware policy organizing server 32)* **(Ackroyd, paragraphs [0029] and [0032])**;

wherein the level of the detected malware event **comprises one of**: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator

attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected *(for example, a particular preferred anti-malware action maybe triggered in response to a detected malware event is to issue a log data message back to the policy organizing server (as an informational or warning malware event); to force an update of malware definition data being used (as a minor malware event); to deal with the malware by disinfecting, repairing or deleting the infected tries or emails as appropriate (as a major malware event) and possibly isolating one or more portions of the computer network from the rest of the computer network in order to isolate a malware outbreak, to protect the rest of the computer network from infection by the malware spreading to them from the already infected department (as a critical malware event))* **(Ackroyd, paragraphs [0030-0032])**;

wherein the level of the event trigger threshold **comprises one of**: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected *(for example, when any of the thresholds has been exceeded or any of the patterns matched, a particular preferred anti-malware action maybe triggered is to issue a log data message back to the policy organizing server (as an informational or warning malware event); to force an update of malware definition data being used (as a minor malware event); to deal with the malware by disinfecting,*

*repairing or deleting the infected files or emails as appropriate (as a major malware event) and possibly isolating one or more portions of the computer network from the rest of the computer network in order to isolate a malware outbreak, to protect the rest of the computer network from infection by the malware spreading to them from the already infected department (as a critical malware event))* **(Ackroyd, paragraphs [0030-0032])**.

However, **Ackroyd** does not **explicitly** teach wherein transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold; wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network.

In an analogous art, **Hansen** teaches a computer network management automatically defining conditions under which a user/administrator is notified of network activity, wherein notification rules would include notification actions specified by the administrator, including executing a script at the server location, reporting the particular event occurrence on a separate event log saved in the network management software, *(i.e., these notification actions could be implemented in real-time and/or eventually)* indicating a change in the state of the device by creating a sound on the host computer, sending an email to a remote address, and sending a page to the administrator's pager when a pre-selected network event occurs *(these notification actions usually being*

*implemented in real-time when a particular predefined network event, to which the threshold has been met or exceeded, i.e., occurs)*. In addition, **Hansen** teaches a corresponding alarm severity class/level can be set to limit triggering of the notification rule based on the extend to which the threshold has been exceeded, for example, **cleared** (or informational), **indeterminate** (or warning), **minor**, **major** and **critical** alarm classes/levels. Specially, the administrator is able to configure the notification function provided by the management software to limit notification, or device status reporting, **to only those instances in which a particular predefined network event occurs** *(i.e., configurable to control an amount of the notifications that are received in real-time to prevent network congestion that adversely affects the usability of the network)* **(Hansen, col. 1, lines 40-43, col. 1, line 57 – col. 2, line 44 and col. 4, lines 20-35)**.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to incorporate the features of including transmitting the notification of the detected malware event in real-time or eventually and the event trigger threshold is configurable to control an amount of the notifications received in real-time so as to prevent network congestion that adversely affects the usability of the network, as disclosed by **Hansen**, into the teachings of **Ackroyd**.

One would be motivated to do so to allow the system to detect/handle malware in a networked environment and to reduce network traffic by limiting notification, or device status reporting to only those instances in which certain pre-selected network events occur **(Hansen, col. 4, lines 20-35)**.

4. As to claim 16, **Ackroyd-Hansen** teaches the method of claim 1, further comprising the step of transmitting an alert to an administrator indicating occurrence of the detected malware in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold *(i.e., creating a sound on the host computer, sending an email to a remote address, and sending a page to the administrator's pager when a certain pre-selected network event occurs)* **(Hansen, C2: L31-44)**.

5. As to claims 49-50, **Ackroyd-Hansen** teaches the method of claim 1, wherein the event trigger threshold is set at a management server by setting policies in the malware management program *(the administrator 12 is able to request the network management software 14 to execute a notification action only when a pre-selected event occurs)* **(Hansen, C4: L20-38)**.

6. As to claim 51, **Ackroyd-Hansen** teaches the method of claim 1, wherein the event trigger threshold is distributed to a plurality of malware agents residing in a plurality of user systems *(malware scanners/agents operating on client computers)*.

7. As to claims 52-53, **Ackroyd-Hansen** teaches the method of claim 1, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until an eventual periodic event transmission or until a request by a management server is received *(the system waits for*

*predetermined regular times to occur at which, i.e., periodically the policy organizing server 32 issues appropriate queries to the database to generate the predetermined reports which are then compared with predetermined patterns and network-wide threshold to trigger predefined anti-malware actions)* **(Ackroyd, paragraphs [0027-0029])**.

8. As to claims 54-59, **Ackroyd-Hansen** teaches the method of claim 1, wherein the level of the event trigger threshold is selected from a ranked set of levels including, from least critical to most critical with progressively greater levels, as follows cleared (or informational), indeterminate (or warning), minor, major and critical (as alarm severity classes/levels) **(Hansen, C1:L49 - C212)**.

9. Claims 17, 32 and 60-70 are corresponding system claims of method claims 1, 16 and 49-59; therefore, they are rejected under the same rationale.

10. Claims 33, 48 and 71-81 are corresponding computer program product claims of method claims 1, 16 and 49-59; therefore, they are rejected under the same rationale.

***(10) Response to Argument***

In the remarks, Applicants argued in substance that

(**A**) Prior Art (the resulting combination of Ackroyd and Hansen) does not disclose or suggest *"an event trigger threshold that is configurable to control an amount of the notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network"*, as claimed in claims 1, 17 and 33.

As to point (**A**), Examiner respectfully submits that **Hansen** teaches an administrator 20 operable to configure the notification function provided by the management software **to limit notification, or device status reporting, to only instances in which a network event occurs** *(i.e., to limit/control notification to only some particular event trigger thresholds)*, wherein a network event represents a change in status of a device being monitored. The administrator 20 is **able to request the network management software to execute a notification action only when a preselected event occurs** *(i.e., executing a notification action according to some predefined event trigger threshold)*. To achieve this notification for specific network occurrences, the network administrator 20 configures the network management software by defining a set of event conditions *(i.e., defining a set of event trigger thresholds)* that describe the particular state upon which notification will occur.

Therefore, the network management software 14 allows the administrator 20 **to receive only notification of certain preselected events that occur on the network** *(i.e., allowing the administrator to control an amount of the notifications to certain preselected events to prevent network congestion that adversely affects the usability of the network)* **(Hansen, col. 4, lines 20-35)**.

It would have been obvious to one having ordinary skill in the art at the time the invention was made to incorporate the features of including an event trigger threshold configurable to control an amount of the notifications received in real-time so as to prevent network congestion that adversely affects the usability of the network, as disclosed by **Hansen**, into the teachings of **Ackroyd**. One would be motivated to do so to allow the system to detect/handle malware in a networked environment and to reduce network traffic by limiting notification, or device status reporting to only those instances in which certain pre-selected network events occur **(Hansen, col. 4, lines 20-35)**.

For the above reasons, it is believed that the rejections should be sustained.

***(11) Related Proceeding(s) Appendix***

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Respectfully submitted,

/Quang N. Nguyen/
Primary Examiner, Art Unit 2441

Conferees,

/Nathan J. Flynn/

Supervisory Patent Examiner, Art Unit 2454

/John Follansbee/

Supervisory Patent Examiner, Art Unit 2451

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, CA 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660